

UNITED STATES PATENT APPLICATION

FOR

METHOD AND APPARATUS FOR VERIFYING THE INTEGRITY OF A MEDIA
KEY BLOCK

Inventor:

Michael S. Ripley

Prepared by:

Blakely, Sokoloff, Taylor & Zafman LLP
12400 Wilshire Blvd., Suite 700
Los Angeles, California 90025
(714) 557-3800

METHOD AND APPARATUS FOR AUTHORIZING
ACCESS TO THE CONTENT OF RECORDABLE MEDIA

COPYRIGHT NOTICE

- 5 Contained herein is material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction of the patent disclosure by any person as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all rights to the copyright whatsoever.

10 FIELD

 This invention relates to static and dynamic information storage and retrieval. More particularly, this invention relates to methods, apparatus and systems for the protection of stored information from unauthorized access.

BACKGROUND

- 15 Information or content may be stored on a wide variety of media. As the speed and convenience of accessing and copying stored information have increased, the threat of unauthorized coping of the information has increased correspondingly. Various schemes have been employed to protect the stored information from unauthorized access. For instance, the content stored on the media may be encrypted with a secret
- 20 key, or keys, known only to devices authorized to access the media. A disadvantage of only one key is the inability to revoke the authorization of a particular device, by changing the key, without revoking the authority of all devices to read the media. Some of the disadvantages of using multiple keys include the potentially large burden of transmitting and storing the keys for each particular device.

- 25 An alternative method developed to protect content from unauthorized copying uses a media key block (MKB) to authorize copying of the content, as described by a publication from 4C Entity, LLC, entitled "CONTENT PROTECTION FOR RECORDABLE MEDIA SPECIFICATION," Revision 0.94 (October 18, 2000). Authorized devices process the MKB to calculate, as described in part below, a media
- 30 key allowing an authorized device to copy the content. The MKB method uses a media unique key to bind encrypted content to the media from which it will be played back.

 An MKB is formatted as a sequence of contiguous records. Each record begins with a record type field, followed by a record length field. In order to process the

MKB, each authorized device receives a set of “n” device keys. The “n” device keys are referred to as Kd_i ($i=0,1,\dots,n-1$). For each device key there is an associated column and row value in the MKB, referred to as column value (Cd_i for $i=0,1,\dots,n-1$) and row value (Rd_i for $i=0,1,\dots,n-1$), respectively. An authorized device will have at most one device key for each column of the MKB. Though, an authorized device may have more than one device key per row.

The device keys and associated row and column values are kept secret. If a set of device keys is compromised, an updated MKB can be released that causes a device with the compromised set of device keys to calculate a different media key than is computed by the remaining compliant devices. In this way, the compromised device keys are “revoked” by the new MKB.

Using its device keys, a device calculates the media key by processing records of the MKB one-by-one from first to last. After processing of the MKB is completed, the device uses the most recently calculated media key value as the final value for the media key. If a device correctly processes an MKB using device keys that are revoked by that MKB, the resulting final media key will have the special value 0H, where H designates a hexadecimal number. This special value will never be an MKB’s correct final media key value, and can therefore always be taken as an indication that the device’s keys are revoked. If a device calculates this special media key value, it stops the authentication, playback, or recording session in progress, and will not use that media key value in any subsequent calculations.

A properly formatted MKB will have exactly one Verify Media Key Record (VMKR) as its first record. The VMKR may also be referred to as validation data. The VMKR contains the hexadecimal value DEADBEEF encrypted with the correct, final media key. The presence of the VMKR is mandatory, but the use of the VMKR by a device is not mandatory. A device may attempt to decrypt the VMKR using its current media key value during the processing of subsequent Records, checking each time for the hexadecimal value DEADBEEF. If the device successfully decrypts the VMKR, the device has already calculated the correct final media key value, and may therefore stop processing the MKB.

A properly formatted MKB will have exactly one calculate media key record (CMKR). Devices must ignore any CMKRs encountered after the first one in an MKB. The CMKR includes a column field. The column field indicates the associated column

value for the device key to be used with this record, as described below. The CMKR also contains encrypted key data in each column corresponding to each of the device key rows. Before processing the CMKR, the device checks that the device has a device key with associated column value $Cd_i = \text{column}$, for some i .

5 If the device does not have a device key with the associated column value, the device ignores the rest of the CMKR. Otherwise, using the value i from the condition above, the device key and $r = Rd_i$, $c = Cd_i$, the device decrypts a media key value from the encrypted key data for row $r = Rd_i$. The resulting media key value becomes the current media key value.

10 A properly formatted MKB may have zero or more conditionally calculate media key records (C-CMKR). The C-CMKR contains encrypted conditional data. In the columns, the C-CMKR contains doubly encrypted key data. If decrypted successfully, as described below, the encrypted conditional data contains the hexadecimal value DEADBEEF and the associated column value for the device key to
15 be used with this C-CMKR. Using its current media key value, the device decrypts conditional data from the encrypted conditional data.

Before continuing to process the Record, the device checks that the following conditions are true: the decrypted conditional data contains the hexadecimal value DEADBEEF and the device has a device key with a newly associated column value (i)
20 decrypted from the conditional data. If any of these conditions is false, the device ignores the rest of the C-CMKR. Otherwise, using the value i from the condition above, the current media key value, and $r = Rd_i$, $c = Cd_i$, the device decrypts the doubly encrypted key data at the associated column in the C-CMKR. The device then decrypts the result of the first decryption of the doubly encrypted data using the
25 device's i -th device key. The resulting media key becomes the current media key value.

As keys are compromised and revoked, the MKB can become quite large, with a size of several megabytes not being unusual. Since many types of media have limited read-only space, it becomes necessary to store the MKB on writeable areas of the media. Storing the MKB on the writeable area creates a vulnerability of the MKB to
30 direct malicious tampering. In such a direct attack, the intent of the tamperer will likely be to substitute an older MKB for the current MKB stored on the media. In the alternative, the tamperer may substitute a portion of an older MKB for a portion of the current MKB stored on the media. Since the older MKB will still contain keys that are

revoked by the current MKB, the substitution will potentially compromise the content protection provided by the current MKB.

Even if the MKB is stored on the readable area of the media, another weakness of the MKB approach is the ability for a man-in-the-middle attack to substitute an older MKB for the current MKB during the attempted processing of the current MKB. In the alternative, the man-in-the-middle attacker may substitute a portion of an older MKB for a portion of the current MKB during the attempted processing of the current MKB. Thus, a man-in-the-middle attack also potentially compromises the content protection provided by the current MKB.

Thus, media without a valid MKB could be read and readers without authorization could read content stored on protected media. In a variation on the MKB approach, a hash value is calculated over the MKB and stored on the read only area of the media. The reader reads the MKB, calculates a hash value of the MKB as read from the media and compares that hash value to the hash value as read from the read only area. Calculating the hash value however imposes an undesirable delay upon the authorization process. Therefore, it is desirable to improve upon the prior art.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a simplified block diagram of an embodiment of the present invention.
Figure 2 is a simplified block diagram of another embodiment of the present invention.
Figure 3 is a simplified block diagram of another embodiment of the present invention.
Figure 4 is a simplified flowchart of a method of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention includes a method, apparatus and system for verifying the integrity of a media key block or other mechanism used to authorize access to content stored on recordable media.

In the following detailed description of the present invention, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be obvious to one skilled in the art that the present invention may be practiced without these specific details. In other instances well known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the present invention.

Herein, certain terminology is used to discuss features of the present invention. For example, content is information programmed by owners or licensees, such as broadcast or cable networks. "Content" can be any form of audible or visual information including business data, news, sports, artistic performances, entertainment, advertising, documentaries, talk, films, videos, cartoons, text, music and graphics.

Media includes any mechanism that provides (i.e., stores and/or transmits) content in a form readable by a machine (e.g., a computer). For example, a machine readable medium includes read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.); etc. Typically, content may be stored in encrypted form on media such as DVDs, CDs, floppy discs, flash memory arrays. Access control comes from the inability of an unauthorized device, or a device having revoked keys, to successfully process the MKB, validate the MKB and then decrypt the content.

A media reader is an electronic device that reads the content from the media. A media reader may also read data other than the content from the media. For instance, media reader may be a DVD drive or player, a CD drive or player, a floppy drive, a digital television, a digital VCR, a CPU of a personal computer, a processor or a circuit coupled to flash memory cells, or any other consumer electronics device capable of accessing content stored on the media. Devices which also write or record to the media, such as CD-RW drives, are also considered media readers.

Referring now to Figure 1, an exemplary embodiment of a media (10) loaded into a media reader (30) is shown. The media reader (30) reads content (1) from the media (10). If the media (10) includes a writeable area (12), the media reader (30) may also write data to the writeable area (12) of media (10). The media reader (30) may be any device capable of reading information stored on a media. The media reader (30) includes microprocessors or other circuits to perform the decryptions, calculations and other processing discussed herein. The media (10) may be any media for storing information.

Media (10) includes a read only area (13) and a media key block (MKB) (11) stored on the media (10). Parts of the MKB (11) may be encrypted and includes a Verify Media Key Record (15) which may also be referred to as "validation data". The validation data (15) is encrypted and contains a pre-selected value. It should be noted

that some media readers (30) decrypt the validation data (15) during the processing of the MKB (11). In such cases, the present invention does not require an additional read operation over the prior art to retrieve the validation data (15).

5 A copy of the validation data (17) is stored on the read only area (13) of the media (10). The copy of the validation data (17) is encrypted in the same manner as the validation data (15) is encrypted. Thus, when the copy of the validation data (17) and the validation data (15) are decrypted the same value should be obtained if no malicious tampering has occurred.

Referring still to Figure 1, the media reader (30) reads information from the media (10). The information that the media reader (30) reads from the media (10) includes the content (1) (after access is authorized), the MKB (31) the media validation data (33) and a copy of the media validation data (35). The media reader (30) decrypts the reader validation data (33), the reader copy of the validation data (35) or both using the media key obtained previously by processing the MKB. If the result of either decryption yields a decrypted value not equal to the preselected value, the media reader (30) refuses to authorize access to the content (1) stored on the media (10). If all of the decrypted values match the preselected value, the media reader (30) continues the authorization process.

It should be noted that the value of a data item as stored on the media (10) and the value of the data item as read by the media reader (30) may differ in an environment in which the content (1) is subject to piracy, direct attacks, man-in-the-middle attacks and other malicious tampering. Therefore, to distinguish between the validation data (15) stored on the media (10) and the validation data (33) read from the media (10) by the media reader (30), the validation data (15) may be referred to as the media validation data (15) and the validation data (33) may be referred to as the reader validation data (33). Similar distinctions can be made between other data items stored on the media (10) and the value of that data item as read by the media reader (30).

The media reader (30) compares the reader validation data (33) and the copy of the reader validation data (35). The comparison may be of either the encrypted values or the decrypted values. Both comparisons may also be made. If the value of the reader validation data (33) and the value of the copy of the reader validation data (35) are equal then the media reader (30) authorizes access to the content (1) stored on the

media (10). If these values are not equal, the media reader (30) refuses to authorize access to the content (1) on the media (10).

Thus, by comparing the reader validation data (33) and the copy of the reader validation data (35) in conjunction with authorizing access, man-in-the-middle devices inserted between the media (10) and the media reader (30) may be detected. The method of authorizing access to the content used in conjunction with the comparison of the two copies of the validation data may be chosen from those methods well known to the art, including for example decrypting a media key from an MKB. A man-in-the-middle alteration of either copy of the media validation data (15 or 17) may be detected by the comparison of the encrypted or decrypted values of the copies of the reader validation data (33 and 35). A man-in-the-middle alteration of both copies of the media validation data will be detected by checking for the pre-selected value in either decrypted copy of the reader validation data, or in both decrypted values.

Referring now to Figure 2, another exemplary embodiment of a media (10) and a media reader (30) of the present invention is shown. In this embodiment, the MKB (51) is stored on the media (10) so as to straddle the boundary between the read only area (13) and the writeable area (12), with the media validation data (55) being stored on the read only area (13). No copy of the validation data is required in this embodiment because the read only nature of the read only area (13) of the media (10) protects the validation data from unauthorized tampering.

Referring now to Figure 3, yet another exemplary embodiment of a media (70) and a media reader (30) of the present invention is shown. In this embodiment, the media (70) includes both the physical media on which the content is stored and a processor or other logic circuit (72). For instance, the media (70) may be a flash memory array including a processor. Another example of a media with a processor is a DVD drive with a CPU to manage the driver. Though, those skilled in the art will recognize that other combinations of media with a processor are obvious. As with other embodiments, the media may also contain a writeable area (12).

A message authentication code may be employed in addition to the validation data discussed previously. To include a message authentication code (MAC) in the present embodiment, the media (70) calculates a media MAC (73) over the copy of the media validation data (17) using a run-time session key established via authentication

and key exchange between the media (70) and a media reader (30). In effect, the media (70) electronically signs the media MKB (11) with the media MAC (73).

The media reader (30) reads the media MAC (73) from the media (70). The media reader (30) also reads the copy of the media validation data (17) and calculates a reader MAC (75) over the copy of the reader validation data (35) using the same algorithm as was used to calculate the MAC (73).

By comparing the reader MAC (75) and the media MAC (73), the media reader (30) makes a second determination of whether authorization for access to the contents of the media (70) should be granted. Should the reader MAC (75) and the media MAC (73) differ, the media reader (30) refuses access to the contents of the media (70). If the two MACs are identical, the media reader (30) allows access to the contents of the media (70). Thus, the media reader (30) checks the electronic signature of the media. The calculation and comparison of the reader and media MACs may occur at any time during the authorization process, including before or after the validation data integrity check is executed.

Thus, a MAC provides another level of protection against man-in-the-middle alterations to the MKB (11). If the man-in-the-middle device alters the copy of the media validation data (17) as the copy of the media validation data (17) is being read from the media (10), the media MAC (73) and the reader MAC (75) will differ.

Another embodiment of the present invention includes a personal computer having a processor and an input/output device such as a DVD drive. A media (10) having a content (1) stored on it is loaded into the input/output device. Upon sensing the presence of the media (10), or upon user command, the processor attempts to access the content stored on the media (10). Thus, the processor of the personal computer acts as a media reader (30) and the input/output device acts as a media (10). The processor may be configured to process the media validation data (15) and the copy of the media validation data (17), as set forth herein. As will be obvious to those skilled in the art, the combination of a media (10) and a media reader (30) form a system for protecting and accessing the content (1).

Referring now to Figure 4, an embodiment of a process (400) for authorizing access to content stored on media of the present invention is shown. Before the media is distributed, the MKB including the media validation data is stored on the media (block 401). The media validation data may be stored on the read only area of the

- media or it may be stored on the writeable area of the media. If the media validation data is stored on the writeable area then a copy of the media validation data is stored on the read only area (block 403). The content is encrypted using the correct media key and then stored on the media before the media is distributed in block 405. In block 407
- 5 the user inserts the media into a media reader or connects the media and media reader as dictated by the form of media employed.

Another embodiment includes a media which encrypts and stores content. In other words, the media of this embodiment may be a content recorder such as a CD-RW drive. Thus, the media may execute block 404.

- 10 Upon sensing the presence of the media or upon a command or request from the user or other device, the media reader reads the media MKB including the media validation data from the media in block 409. If a copy of the media validation data has been previously stored on the read only area of the media, the media reader also reads the copy of the media validation data from the media in block 411.

- 15 The media reader may then compare the encrypted value of the reader validation data read from the media with the encrypted value of the copy of the reader validation data read from the media. If the two values are different the media reader denies authorization to access the content in block 414. Otherwise, the authorization process may continue with block 415.

- 20 In blocks 415 and 417, the media reader decrypts the reader validation data read from the media and the copy of the reader validation data read from the media. The media reader may then compare the decrypted values of the reader validation data and of the reader copy of the validation data, as in block 419 using the media key obtained by processing the MKB. If the two values are different the media reader denies
- 25 authorization to access the content. Otherwise, the authorization process continues with block 420.

- In block 420, the media reader compares either the decrypted value of the reader validation data or the decrypted value of the copy of the reader validation data to the pre-selected value. In the alternative, the reader may compare both the decrypted
- 30 reader validation data and the decrypted copy of the reader validation data to the pre-selected value. If any one of the comparisons fails, then the media reader denies authorization to access the content.

In blocks 421 and 423, the media and media reader establish a shared session key in any manner known to the art. The media reader, in block 425, calculates a reader MAC over a reader hash value of the reader MKB read from the media. The media, in block 427, likewise calculates a media MAC over a media hash value of the media MKB. In blocks 426 and 429, the driver then reads the media MAC from the media and compares it to the reader MAC. If the two values are different the media reader denies authorization to access the content. Otherwise, the driver may authorize access to the content or may process the MKB, as shown in block 431.

Another exemplary embodiment includes processing the MKB to obtain the correct media key; decrypting the validation data with the media key; verifying that the validation data contains the correct preselected value; and comparing the encrypted value of the validation data in the MKB with the encrypted validation data over which a MAC has been successfully calculated by the device and reader. Another exemplary embodiment includes successfully calculating a MAC over the validation data; decrypting the validation data stored on the read only area of the media; and verifying that the validation data contains the correct preselected value. Yet another embodiment includes calculating and comparing the MACs before reading the two copies of the validation data. Thus, when the reader reads either copy of the validation data the MAC may accompany the validation data.

Instructions to execute the process described above may be stored on a machine readable medium. The machine-readable medium includes any mechanism that provides (e.g., stores and/or transmits) information in a form readable by a machine (e.g., a computer). For example, a machine-readable medium includes read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.); etc. Those skilled in the art will recognize that a media may be used to store instructions to execute the process described above, and a medium may be used to store or transmit content.

Since a man-in-the-middle attack cannot alter the read only copy of the validation data, the present invention will detect such an attack. Furthermore, if the present invention is used in conjunction with an authorization scheme such as an MKB, man-in-the-middle attacks, which attempt to alter the MKB as the MKB is read from

- the media, will likewise be detected. In addition, since the present invention may involve as few calculations as a decryption of a relatively small validation data, as opposed to calculating a hash value over an entire MKB, the present invention provides much quicker verification of the integrity of the MKB. Moreover, the present invention
- 5 provides improved content protection over the prior art.

While the present invention has been described in particular embodiments, the present invention should not be construed as limited by such embodiments, but rather construed according to the claims that follow below.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2